khaledyassinkh@gmail.com

بسم الله الرحمن الرحيم
قال تعالى: "و قل ربي زدني علما"

ملاحظة: إذا كان ضمن الخيارات خيار "لا يوجد" هذا يعني أن جميع الإجابات السابقة خاطئة

1- أي من الجمل التالية تشير إلى تهديد أمني security threat :
- A عدم إعداد قائمة النفاذ في الجدار الناري بشكل مناسب
- B عدم إعداد نقطة النفاذ في الشبكة المحلية اللاسلكية(wireless LAN access point) بشكل مناسب
- **C (*)تعديل المعطيات**
- D لا يوجد حراس للتدقيق في بطاقات الدخول
- E عدم الإبلاغ عن بطاقات الدخول المفقودة

2- أي من الجمل التالية تشير إلى نقطة ضعف أمنية (security vulnerability)؟
a. الدخول خلف شخص مخول
b. العمل بشكل غير مخول على حاسب بوضعية logged-in.
c. تغيير إعدادات النظام (Change system setting) .
d. (*)ملفات مهمة غير ممحوة بشكل مناسب (Sensitive file are not erased properly) .
e. الدخول عبر نقاط الدخول في الشبكات اللاسلكية (Intrusion through wireless LAN's access point)

3- أي من الأهداف الأمنية تستطيع الحد من أضرار هجوم التحري (Snooping attack) عن المعلومات؟
a. السرية (Confidentiality)
b. التكاملية (Integrity)
c. التحكم بالنفاذ (Access control)
d. وثوقية كيان (Entity authentication)
e. (*)a. و c.

4- أي من الآليات الأمنية التالية تستطيع إيقاف هجوم إعادة الإرسال(Replay attack) ؟
a. بروتوكول تحدٍ –جواب لتبادل الوثوقية (Challenge-response authentication exchange protocol)
b. استخدام كلمات مرور وحيدة الاستخدام (One-time passwords) في عملية الوثوقية
c. استخدام كلمات مرور قوية (strong passwords) في عملية الوثوقية
d. (*)استخدام الشهادات (Certificate) في عملية الوثوقية
e. b. و c.

5- أي من الآليات الأمنية التالية تستطيع إيقاف هجوم إعادة الإرسال(Replay attack) ؟
a. بروتوكول تحدٍ –جواب لتبادل الوثوقية (Challenge-response authentication exchange protocol)
b. استخدام كلمات مرور وحيدة الاستخدام (One-time passwords) في عملية الوثوقية
c. (*)إرفاق الطابع الزمني (Timestamp) مع الرسائل
d. استخدام كلمات مرور قوية (Strong passwords) في عملية الوثوقية
e. b. و c.

6- أي من الأهداف الأمنية تمنع الأشخاص المخولين(Authorized persons) من التلاعب بقواعد المعطيات؟
a. وثوقية كيان (Entity Authentication)
b. (*) التخويل (Authorization)
c. التوافرية (Availability)
d. السرية (Confidentiality)
e. a. و b.

7- أي من الأهداف الأمنية التالية تمنع هجوم رفض/حجب الخدمة(Denial of service attack)؟
a. وثوقية كيان (Entity Authentication)
b. التحكم بالنفاذ (Access Control)
c. السرية (Confidentiality)
d. عدم النكران (Non-repudiation)
e. (*)لا يوجد

8- إلى أي من تقنيات الإجراءات الأمنية التالية ينتمي التوقيع الرقمي :
a. الوقاية
b. (*)الكشف

c. الاسترجاع
d. a و c
e. لا يوجد

9- إلى أي من تقنيات الإجراءات الأمنية ينتمي الجدار الناري:
a. الوقاية
b. الكشف
c. الاسترجاع
d. a(*) و b.
e. لا يوجد

10- إلى أي من أنواع الهجوم ينتمي إلحاق الضرر بكابلات الشبكات:
a. المقاطعة(*)
b. تعديل
c. انتحال الشخصية
d. التكرار
e. a. و b.

11- أي من المعميات Ciphers التالية تعد من أكثر المعميات تسبباً لانتشار الأخطاء:
a. AES بالنمط CBC
b. **3DES(*) بالنمط CBC**
c. DES بالنمط CBC
d. DES بالنمط ECB
e. One-time pad

12- أي من المعميات Ciphers التالية تعد من أقل المعميات تسبباً لانتشار الأخطاء:
a. AES بالنمط CBC
b. 3DES بالنمط CBC
c. DES بالنمط CBC
d. DES بالنمط ECB
e. **One-time pad (*)**

13- أي من أنماط التشغيل (Modes of Operations) تستطيع أن تسبب أكبر عدد من عمليات فك التشفير الخاطئة لنص منقول عبر الشبكة و مكون من عدد كبير من الكتل؟
a. ECB –Electronic Code Book
b. CBC –Cipher Block Chaining(*)
c. CFB –Cipher Feedback
d. a. و c.
e. جميع ما سبق

14- أي من المعميات Ciphers التالية تعد الأنسب في حماية الاتصال بين لوحة المفاتيح ووحدة المعالجة الرئيسية؟
a. DES بالنمط CBC
b. DES(*) بالنمط CFB
c. DES بالنمط ECB
d. جميع ما سبق
e. لا يوجد

15- أي من المعميات الكتلية (Block Cipher) التالية تمتلك أطول مفتاح تشفير؟
a. AES(*)
b. IDEA
c. 3DES
d. One-time pad
e. a. و b.

16- أي من المعميات التالية تسمح لمرسل الرسالة المشفرة تحديد طول كتلة التشفير؟
a. IDEA
b. RSA
c. AES
d. EL GAMAL
e. b.(*) و d.

17- أي من المعميات التالية لا يستطيع إلا مستقبل الرسالة المشفرة تحديد طول كتلة التشفير ؟
a. IDEA
b. RSA
c. AES
d. EL Gamal
e. (*)b. و d.

18- أي من المعميات التالية يمكن أن تعطي تشفير مختلف للرسالة نفسها في كل مرة نشفر بها هذه الرسالة:
a. IDEA
b. RSA
c. AES
d. EL Gamal(*)
e. لا يوجد

19- [DOS ينتمي إلى :
a. Web Server
b. Web Browser
c. Communication Channel
d. (*)a. و c.
e. لا يوجد

20- باستخدام Challenge Response لإرسال رسالة بين شخصين متباعدين جغرافيا أي التقنيات التالية هي الأسوأ :
a. Nonce
b. Timestamp(*)
c. Sequence number
d. b. و c.
e. لا يوجد

ملاحظة هامة: Nonce هو نفسه Time stamp (و بلغة أدق قد يحوي Timestamp) لذا إذا كان من ضمن الخيارات خيارا يجمعهما نختار هذا الخيار و إلا نختار Timestamp

21- أي من الجمل يحققه تعريف Trojan:
a. (*)يخدع المستخدم
b. ينسخ ويكرر نفسه
c. ينتشر باستغلال الثغرات الأمنية
d. لا يحتاج لبرنامج مضيف
e. a. و d.

22- أي من الجمل يحققه تعريف Virus:
a. يخدع المستخدم
b. ينسخ و يكرر نفسه عبر الشبكة
c. ينتشر باستغلال الثغرات الأمنية
d. لا يحتاج لبرنامج مضيف
e. (*)لا يوجد

ملاحظة هامة: يحتاج الفيروس و التروجان إلى برنامج مضيف لكي ينتشرا بينما الدودة تنتشر بشكل تلقائي عبر وصلات الشبكة باستغلال الثغرات الأمنية

23- أي من البرمجيات الخبيثة تنتشر باستغلال الثغرات الأمنية
a. Trojan
b. Virus
c. Worm(*)
d. لا يوجد

24- أي من العبارات التالية صحيحة فيما يتعلق بـ Trojan:
a - توعية المستخدمين يخفف من خطر انتشار حصان طروادة
b - حصان طروادة أقل خطر من الفيروس

c - يعتمد حصان طروادة على برمجيات أخرى في الانتشار
d - a. و b.
e - (*)a. و c

ملاحظة: الفيروس يكرر نفسه بينما التروجان لا يكرر نفسه و كلاهما ينتشران عن طريق إلحاق نفسهما ببرنامج مضيف

25- أي من الجمل التالية تحققها تعريف الفيروس:
a. يعتمد على نفسه في الانتشار
b. نوع من أنواع البرمجيات الخبيثة
c. يحتاج لبرنامج مضيف
d. كل ما سبق
e. (*)b. و c.

26- إلى أي من تقنيات الإجراءات الأمنية التالية ينتمي نظم كشف التطفل IDS (intrusion detection system):
a. الوقاية
b. (*)الكشف
c. الاسترجاع
d. a و c
e. لا يوجد

27- ما هي التقنية التي تؤمن عدم النكران(ملاحظة يا حبيبي هنا عدم نكران المرسل أنه أرسل الرسالة و ليس المستقبل أنه استقبل الرسالة تحياتي للمرسل و المستقبل) :
a. (*) التوقيع الرقمي
b. MAC
c. Encryption
d. Hash
e. لا يوجد

28- يرسل الكيان A رسالة موقعة إلى الكيان B ما الذي يجب أن يتوفر لدى الطرف A (المرسل):
a. خوارزمية التشفير و المفتاح الخاص ب A
b. خوارزمية التوقيع و المفتاح العام بـB
c. (*) خوارزمية الهاش و خوارزمية التوقيع و المفتاح الخاص بـA
d. MAC + مفتاح مشترك بين الطرفين
e. خوارزمية التوقيع و المفتاح الخاص بـA

29- يرسل الكيان A رسالة موقعة و سرية إلى الكيان B ما الذي يجب أن يفعله الطرف A (المرسل):
a. (*) يوقع ثم يشفر (ملاحظة هنا يتم توقيع هاش الرسالة (ملخص الرسالة) ثم يشفر الرسالة مع التوقيع)
b. يشفر ثم يوقع
c. يحتوي خوارزمية التشفير و المفتاح العام لـB
d. b. و c.

30- ما هو حجم المفتاح الغير مستخدم في الخوارزميات التناظرية الكتلية(Block ciphe):
a. 56
b. 128
c. 130
d. 192
e. لا يوجد

31- فيما يتعلق بسياسة التحكم بالنفاذ ما هي أفضل سياسة من وجهة النظر الإدارية:
a. MAC
b. DAC
c. (*)RBAC
d. CBAC

32- فيما يتعلق بسياسة التحكم بالنفاذ ما هي أفضل سياسة تؤمن المستويات الأمنية:
a. (*)MAC
b. DAC
c. RBAC
d. CBAC

33- فيما يتعلق بسياسة التحكم بالنفاذ ما هي السياسة التي لا تستطيع منح صلاحيات للآخرين:
a. MAC

b. DAC
c. RBAC
d. CBAC
e. (*)لا يوجد

34- ما هو الذي لا يتحمله إداري النظام(المخدم) server Administrator :
a. محو الوب(شو يعني ؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟)
b. DOS(*)
c. منح الصلاحيات
d. حذف الصلاحيات
e. لا يوجد

35- في دورة حياة النظام SDLC الكشف عن نقاط الضعف في أي مرحلة تتم:
a. Investigation
b. Analysis
c. Design
d. Implementation
e. Maintenance(*)

36- في دورة حياة النظام SDLC تدريب العاملين على التكنولوجيا في المؤسسة:
a. Investigation
b. Analysis
c. Design(*)
d. Implementation
e. Maintenance

37- في دورة حياة النظام SDLC متى تعلن المؤسسة مسؤوليتها عن المشروع:
a. Investigation(*)
b. Analysis
c. Design
d. Implementation
e. Maintenance

38- في دورة حياة النظام SDLC إدارة المخاطرة متى تتم:
a. Investigation
b. Analysis(*)
c. Design
d. Implementation
e. Maintenance

39- في دورة حياة النظام SDLC تغليف المشروع متى تتم:
a. Investigation
b. Analysis
c. Design
d. Implementation(*)
e. Maintenance

40- أي من بروتوكولا SSL يقدم خدمات أمنية:
a. Handshake protocol
b. SSL Alert protocol
c. Ssl Change Cipher Spec protocol
d. SsL record protocol(*)
e. كل ما سبق

41- أي من التقنيات التالية تمنع إعادة إرسال الرسالة؟
a. التشفير
b. التحكم بالنفاذ
c. السرية
d. Sequence number(*)
e. a. و c.

42- عند التشفير بالمفتاح العام للمستقبل فإن ذلك يحقق:
a. السرية
b. التكاملية
c. التحكم بالنفاذ
d. الوثوقية
e. (*)a. و b.

43- عند يوقع المرسل على رسالة باستخدام مفتاحه الخاص فإن ذلك يؤمن:
a. عدم نكران المرسل أنه مرسل الرسالة
b. التوقيع الرقمي
c. السرية
d. a. و b.
e. b. و c.

44- عند ما يوقع المرسل على رسالة باستخدام مفتاحه العام فإن ذلك يؤمن:
a. السرية
b. التوقيع الرقمي للمستقبل
c. التكاملية
d. الوثوقية
e. لا يوجد

45- عند يوقع المرسل على رسالة باستخدام مفتاحه الخاص فإن ذلك يؤمن:
a. التكاملية
b. التوقيع الرقمي
c. السرية
d. a. و b.
e. b. و c.

46- أي حقل لا ينتمي لحقول الـ certificate الموصفة بالمعيار x.509:
a. version
b. serial number
c. signature algorithm
d. ISSUER name
e. لا يوجد

47- هجوم DOS هو تهديد ينتهك:
a. Confidentiality
b. Integrity
c. Availability(*)
d. Access control
e. d. و c.

48- متى تتم عملية الانتقال إلى disaster recovery plan:
a. عند اكتشاف الحادث
b. عند وقوع الحادث
c. (*)عندما يتحول الحادث إلى كارثة
d. لا يوجد

49- في أي صنف من السياسات الأمنية يوضع توصيف تشكيل وصيانة الأنظمة الحاسوبية:
a. EISP
b. ISSP
c. SYS SP
d. لا يوجد

50- عكس xor هو:
a. And
b. Or
c. Xor
d. لا يوجد

51- أي من الأهداف الأمنية تمنع الأشخاص المخولين من التلاعب بقواعد المعطيات:
a. التخويل
b. التحكم بالنفاذ
c. السرية
d. التوافرية
e. (*)a. و b.

52- أي من التهديدات الأمنية لا تعتبر أساسية في نظام بريد إلكتروني:
a. نكران الإرسال
b. (*)إعادة الإرسال
c. تعديل الرسالة
d. قراءة الرسالة من الآخرين
e. التنصت

53- أي من التالي تمنع مستقبل الرسالة من نكران استقباله للرسالة:
a. التوقيع الرقمي
b. استخدام hash مع MAC
c. استخدام مفتاح المستقبل العام لتوقيع الرسالة و مفتاحه الخاص لفك الرسالة
d. استخدام مفتاح المرسل الخاص لتوقيع على الرسالة و مفتاح العام للمستقبل لتشفير الرسالة
e. (*)استخدام عملية الشهادات بالاعتماد على طرف ثالث موثوق (ويجب على كلا الطرفين استخدام الشهادات)

54- إذا اردنا تحقيق أفضل تطبيق للسياسة الأمنية المتبعة في مؤسسة ما على أي مستوى كان يجب أن يشارك لتحقيق ذلك:
a. فريق أمن نظم المعلومات
b. مجموعة نظم التشغيل
c. المسؤول administrator
d. المستخدمين في هذه المؤسسة
e. (*)كل ما سبق

55- باستخدام Challenge Response لإرسال رسالة بين شخصين متباعدين جغرافيا أي التقنيات التالية هي الأسوأ من حيث التخزين(تحتاج لتخزين) :
a. Nonce
b. **Timestamp**
c. Sequence number
d. لا يوجد

56- باستخدام Challenge Response لإرسال رسالة بين شخصين متباعدين جغرافيا أي التقنيات التالية التي تؤمن حماية ضد إعادة إرسال الرسالة:
a. Nonce
b. **Timestamp**
c. Sequence number
d. a. و c.
e. (*)كل ما سبق

57- أي من التقنيات التالية تعد الأنسب لتأمين خدمة سلامة المعطيات integrity :
a. التوقيع الرقمي
b. (*)MAC كود وثوقية رسالة
c. التشفير المناظر
d. التشفير اللامتناظر
e. a. و c.

ملاحظة هامة: هذا السؤال يقول من الأنسب نحن نعلم أن التوقيع الرقمي يحقق التكاملية عن طريق تشفير هاش الرسالة باستخدام مفتاح المرسل الخاص و خوارزمية التوقيع و عند الطرف المستقبل يقوم بتطبيق خوارزمية التوقيع باستخدام مفتاح المرسل العام هنا تم الثوثق من المرسل ثم يقوم المستقبل بتطبيق الدالة الهاشية التي طبقها المرسل و في حال التساوي يعني حققنا التكاملية ولكن هذه الطريقة يستطيع أي شخص تطبيقها لأن مفتاح المرسل العام معروف أماMAC

فييتم بتطبيق الدالة الهاشية لتحقيق التكاملية باستخدام مفتاح مشترك بين المرسل و المستقبل و الفكرة واضحة و التوقيع الرقمي أبطئ و كذلك التشفير يحقق التكاملية و لكن هناك بطئ بسبب عمليات التشفير و فك التشفير

58- اختر العبارة الصحيحة:
a - الخوارزميات التناظرية أسرع من الخوارزميات اللاتناظرية
b - توابع الهاش في المعالجة أسرع من الخوارزميات التناظرية
c - توابع الهاش لا تنتج بفردها عملية وثوقية وتكاملية للرسالة
d - (*)كل ما سبق
e - a. و b.
ملاحظة: الهاش لوحدها لا تحقق إلا التكاملية
59- أبسط مثال يمكن أن نعبر عنه للهجوم رفض/حجب الخدمة DOS (denial of service attack) هو:
a. (*)قطع الكبل
b. تعديل المعلومات
c. انتحال الشخصية
d. نكران الإرسال
e. كل ما سبق
60- أي من الهجمات التالية لا يستطيع firewall أن يمنعها:
a. هجوم port scan
b. هجوم SYN Flooding
c. هجوم Application Content
d. هجوم IP address
e. (*)هجوم social engineering
61- الدالة XOR دالة منطقية :
a. تنفع للتشفير بذاتها
b. لا تنفع للتشفير
c. (*)لا تنفع للتشفير بذاتها بل يجب أن تستخدم ضمن طريقة ما
d. a. و b.
e. كل ما سبق
62- أذا كان لدينا كيان A يريد إرسال رسالة موقعة للكيان B :
a. (*)يقوم الكيان A بإدخال الرسالة إلى إحدى التوابع الهاشية وبأخذ الكيانA هذا الهاش ويقو بتشفيره بمفتاحه الخاص و هكذا يحصل الكيان A على التوقيع و يرسل الرسالة بعد إضافة التوقيع لها و يرسلها إلى الكيانB
b. يقوم الكيانB بإدخال الرسالة إلى إحدى التوابع الهاشية وبأخذ الكيانA هذا الهاش ويقو بتشفيره بمفتاحه الخاص و هكذا يحصل الكيان A على التوقيع و يرسل الرسالة بعد إضافة التوقيع لها و يرسلها إلى الكيانB
c. يقوم الكيان A بإدخال الرسالة إلى إحدى التوابع الهاشية وبأخذ الكيانB هذا الهاش ويقو بتشفيره بمفتاحه الخاص و هكذا يحصل الكيان A على التوقيع و يرسل الرسالة بعد إضافة التوقيع لها و يرسلها إلى الكيانB
d. يقوم الكيان A بإدخال الرسالة إلى إحدى التوابع الهاشية وبأخذ الكيانA هذا الهاش ويقو بتشفيره بمفتاحه العام و هكذا يحصل الكيان A على التوقيع و يرسل الرسالة بعد إضافة التوقيع لها و يرسلها إلى الكيانB
e. يقوم الكيان A بإدخال الرسالة إلى إحدى التوابع الهاشية وبأخذ الكيانB هذا الهاش ويقو بتشفيره بمفتاح الخاص للكيان B و هكذا يحصل الكيان A على التوقيع و يرسل الرسالة بعد إضافة التوقيع لها و يرسلها إلى الكيانB

63- بعد إرسال الرسالة من الكيان A إلى الكيان B يقوم الكيان B بما يلي ليتأكد من مصدرها:
a. (*)يقوم الكيان B بفك تشفير التوقيع باستخدام مفتاح A العام و الناتج يكون الهاش ويكون عرف أن المرسل هو الكيان A و ليس أحد آخر
b. يقوم الكيان A بفك تشفير التوقيع باستخدام مفتاح B العام و الناتج يكون الهاش ويكون عرف أن المرسل هو الكيان A و ليس أحد آخر

c. يقوم الكيان B بفك تشفير التوقيع باستخدام مفتاح A الخاص و الناتج يكون الهاش ويكون عرف أن المرسل هو الكيان A و ليس أحد آخر
d. يقوم الكيان B بفك تشفير التوقيع باستخدام مفتاحه الخاص و الناتج يكون الهاش ويكون عرف أن المرسل هو الكيان A و ليس أحد آخر

khaledyassinkh@gmail.com

64- بعد إرسال الرسالة من الكيان A إلى الكيان B و بعد أن تأكد الكيان B أن A هو المرسل يريد أن يتحقق من سلامة معطيات الرسالة و الخطوات تكون:

a. (*)يقوم الكيان B بتطبيق الدالة الهاشية التي طبقها الكيان A على الرسالة و في حال التساوي يكون عرف أن الرسالة لم تتغير أثناء إرسالها
b. يقوم الكيان B بفك تشفير التوقيع باستخدام مفتاحه الخاص و الناتج يكون الهاش ويكون عرف أن المرسل هو الكيان A و ليس أحد آخر
c. يقوم الكيان B بفك تشفير التوقيع باستخدام مفتاح A الخاص و الناتج يكون الهاش ويكون عرف أن المرسل هو الكيان A و ليس أحد آخر
d. لا يوجد

65- اختر العبارة الصحيحة:

a. التشفير الدفقي أفضل من التشفير الكتلي
b. التشفير الدفقي أسرع من التشفير الكتلي
c. التشفير الدفقي والتشفير الكتلي يستخدمان المفتاح الذي يستخدم في التشفير لفك التشفير
d. الكود الذي يكتب بالتشفير الكتلي أكبر بكثير من الكود الذي يكتب بالتشفير الدفقي
e. (*)كل ما سبق

66- أي من الأهداف الأمنية لا يمكن أن تتحقق عن طريق التوقيع الرقمي بدون وسيط ثالث:

a. الوثوقية
b. (*)السرية
c. التكاملية
d. a. و b.
e. b. و c.

67- اختر العبارة الصحيحة:

a. التشفير الكتلي و التشفير الدفقي يستخدمان المفتاح نفسه للتشفير وفك التشفير
b. التشفير اللامتناظر أسرع من التشفير الكتلي
c. الكود الذي يكتب بالتشفير الدفقي أكبر بكثير من الكود الذي يكتب بالتشفير الكتلي
d. يعتمد التشفير الدفقي في الأمن على قوة تابع التشفير
e. كل ما سبق

68- اختر العبارة الصحيحة :

a. 3DES أبطئ بثلاث مرات من DES
b. 3DES أكثر أماناً بثلاث مرات من DES
c. مفتاح التشفير في خوارزمية 3DES يساوي ثلاث أضعاف مفتاح التشفير في DES
d. عدد اللفات في DES هو 16
e. (*) كل ما سبق

69- في دورة حياة النظام SDLC تطوير السياسة الأمنية متى تتم:

a. Analysis
b. Design (*)
c. Implementation
d. Investigation

70-عدد اللفات rounds في خوارزمية AES هو:

a. (*)حسب Key size
b. 12
c. 14

71- ما هي التقنية التي تضمن لنا وثوقية كيان بشكل فيزيائي:

a. التشفير
b. التوقيع الرقمي
c. MAC
d. استخدام الشهادات في عملية الوثوقية
e. (*)لا يوجد

72- ما هي التقنية التي تضمن لنا وثوقية كيان بشكل فيزيائي:

a. Biometrics(*)
b. Token
c. Password

d. Ticket
e. كل ما سبق

73- ما هي التقنية التي تحتاج لوسيط ثالث موثوق:
a. Biometrics
b. Token
c. Password
d. Ticket(*)
e. كل ما سبق

74- message authentication وثوقية الرسالة يستطيع أن يُحققها:
a. التوقيع الرقمي digital signature
b. MAC كود وثوقية رسالة
c. Message encryption
d. b و c.
e. (*)كل ما سبق

75- التوقيع الرقمي digital signature يستخدم لتحقيق:
a. Authentication
b. Non-repudiation
c. Integrity
d. (*)كل ما سبق
e. b و c.

76- spam البريد المزعج قد يكون من البرمجيات الخبيثة(قد يسبب Dos Attack) ما هي الحلول المكنة :
a. إيقاف Active content او أي attachmentمن نمط معين من قبل administrator
b. أن يمنع mail server عملية spam
c. استخدام القوائم السوداء black list
d.(*) كل ما سبق
e. a و c.

77- إلى أي من تقنيات الإجراءات الأمنية ينتمي التشفير بالمفتاح العام:
a. الوقاية
b. الكشف
c. **(*)الاسترجاع**
d. a و b.
e. لا يوجد

78- إلى أي من تقنيات الإجراءات الأمنية ينتمي التشفير بالمفتاح الخاص:
a.الوقاية b. التوقيع c.الكشف d. a و b. e. **(*)b. و c.**

79- إلى أي من تقنيات الإجراءات الأمنية ينتمي التشفير بالمفتاح المشترك:
a.الوقاية bالتحقق(الكشف) c.الاسترجاع d. a و b. e. b. و c.

80- خرج خوارزمية الهاش(ملخص الرسالة) SAH-1 هو:
a. 256 bits
b. 20 bytes
c. 130 bits
d. 160 bits
e. (*)b. و d.

81- من نقاط الضعف في Firewall هي:
a. لا يمنع أي شيء مسموح
b. هو فعال بفعالية القواعد التي ينفذها
c. لا يحمي سياسة أمنية ضعيفة
d. لا يحمي من أي Traffic لا يمر عبره
e. (*)كل ما سبق

82- ما هو الأمر الذي نستطيع من خلاله إعطاء أمر الامتياز للمستخدمين فيSQL من دون امتيازات للمنح:
a. Grant(*)
b. *Grant Option*

c. WITH GRANT
d. كل ما سبق
e. a. و b.

83- الأمر Revoke يمكن :
a. المستخدم من سحب الامتيازات التي منحها
b. لدى تنفيذ الأمر Revoke يخسر المستخدم الامتيازات التي منحت له، إلا إن كان قد استقبلها من قبل مستخدم آخر
c. (*)كل ما سبق

84- من سياسات التحكم بالنفاذ التي يتم النفاذ إلى الأغراض تتعلق بهوية الموضوع و قواعد التخويل بشكل رئيسي هي:
a. MAC
b. DAC(*)
c. RBAC
d. CBAC
e. كل ما سبق

85- عند إرسال رسالة موقعة و مشفرة(سرية) من المرسل إلى المستقبل ما الذي الخطوات التي يقوم بها المستقبل ليتأكد من مصدر و تكاملية الرسالة
a. (*)يفكك تشفير الرسالة باستخدام مفتاحه الخاص و خوارزمية فك التعمية ثم يطبق خوارزمية التأكيد (التوقيع) باستخدام مفتاح A المعلن ثم يطبق الدالة الهاشية التي طبقها المرسل على الرسالة ويقارن نتيجة الهاش و في حال التساوي يكون قد تحققت التكاملية
b. يفكك تشفير الرسالة باستخدام مفتاحه العام و خوارزمية فك التعمية ثم يطبق خوارزمية التأكيد (التوقيع) باستخدام مفتاح A المعلن ثم يبق الدالة الهاشية التي طبقها المرسل على الرسالة و في حال الاختلاف يكون تعديل حصل على الرسالة
c. يفكك تشفير الرسالة باستخدام مفتاحه الخاص و خوارزمية فك التعمية ثم يطبق خوارزمية التأكيد (التوقيع) باستخدام مفتاح A الخاص
d. يفكك تشفير الرسالة باستخدام مفتاحه العام و خوارزمية فك التعمية ثم يطبق خوارزمية التأكيد (التوقيع) باستخدام مفتاح A الخاص

86- أي من بروتوكولات SSL تقوم بالتحقق من هوية web browser:
a. Ssl handshake protocol(*)
b. Ssl record protocol
c. Ssl change cipher protocol
d. Ssl alert protocol
e. كل ما سبق

87- أي من بروتوكولات SSL تقوم بالتحقق من هوية web server:
a. Ssl handshake protocol(*)
b. Ssl record protocol
c. Ssl change cipher protocol
d. Ssl alert protocol
e. كل ما سبق

88- أي من بروتوكولات SSL تقوم بعملية تبادل للمفاتيح لتحقيق الوثوقية و السرية:
a. Ssl handshake protocol(*)
b. Ssl record protocol
c. Ssl change cipher protocol
d. Ssl alert protocol
e. كل ما سبق

89- أي من بروتوكولات SSL تقوم بعملية الإشارة إلى الأخطاء التي قد تحدث في عمليات التشفير أو لضغط :
a. Ssl handshake protocol
b. Ssl record protocol

c. Ssl change cipher protocol
d. Ssl alert protocol(*)
e. كل ما سبق

90- تعتمد خوارزمية DES على مفهوم أساسي:
a. Product cipher concept
b. Feistel concept
c. (*)كل ما سبق

91- أي من بروتوكولات SSL تقوم تستخدم للاتفاق على خوارزميات التشفير و authentication:
a. Ssl handshake protocol(*)
b. Ssl record protocol
c. Ssl change cipher protocol
d. Ssl alert protocol
e. كل ما سبق

92- أي من العبارات التالية تشكل خدمة أمنية:
a. يجب منع الوصول إلى مخدم ftp
b. استخدام VPN(virtual private network) للوصول للشبكة الدخلية
c. استخدام ترشيح بالاعتماد على البوابات و العناوين
d. حصر استخدام Email بإداري واحد
e. (*)استخدام AES لتشفير المعطيات المتبادلة بين المستخدمين و مخدم المعطيات

93- أي من العبارات التالية لا تشكل جزءا من سياسة أمنية:
a. يجب منع الوصول إلى مخدم ftp
b. استخدام VPN(virtual private network) للوصول للشبكة الدخلية
c. استخدام ترشيح بالاعتماد على البوابات و العناوين
d. حصر استخدام Email بإداري واحد
e. (*)استخدام AES لتشفير المعطيات المتبادلة بين المستخدمين و مخدم المعطيات

94- متى نضع firewall :
a. Instigation
b. Analysis
c. Design(*)
d. Implementation
e. Maintenance

95- إذا أردنا باستخدام ssl record protocol تشفير المعطيات المتبادلة بين الجهازين A و B فإن عدد المفاتيح المشتركة بينهما يجب أن يكون على الأقل هو:
a. 1
b. 2
c. 3(*)
d. 4
e. 5

96- أي من الأمور التالية تسبب اختراق خصوصية المستخدم:
a. Cookies(*)
b. Java code
c. Html code
d. Code signing
e. Sand box

97- snort هو عبارة عن :
a. (intrusion detection system) IDS(*)
b. Packet filtering
c. Application gateway
d. Stateful packet inspection
e. Netscreen

98- حماية كود java applets تتم عبر تقنية
a. cookies
b. Java code
c. Html code
d. Code signing
e. Sand box(*)

99- حماية كود activex تتم عبر تقنية :
a. cookies
b. Java code
c. Html code
d. Code signing(*)
e. Sand box

100- أي من العبارات التالية صحيحة:
a. Mobile code تشكل خطرا على web browser
b. Mobile code هو كود تنفيذي
c. يمكن لبرنامج خبيث أن يشكل خطرا على web browser و web server
d. Cookies تشكل خطرا على web browserوليس على web server
e. (*)كل ما سبق

101- ما هي الخاصية التي لا تمنع و لا تعالج الخطر:
a. الرفض
b. التخفيف
c. إرسالها إلى غيرها
d. (*)القبول بها
e. كل ما سبق

102- ما هي الخاصية التي تخفف من الخطر:
a. التجنب
b. التخفيف
c. الانتقال
d. القبول بها
e. **a. و b.**

103- الخوارزمية الهاش التي تستخدمها خوارزمية EL GAMAL(هذه الخوارزمية نسبة لمخترعها للعالم العربي المصري طاهر الجمل) في توقيع الرسالة :
a. SHA-1(*)
b. MD5
c. HMAC
d. a. و b.
e. c. و a.

104- تعتمد خوارزمية DSS (digital signature standard) في عملية التوقيع الرقمي على:
a. خوارزمية الهاش(تابع ضغط)
b. عدد عشوائي يستخدم لمرة واحدة
c. المفتاحين العام و الخاص للمرسل و معاملات عامة
d. (*)كل ما سبق
e. a. و b.

105- تعتمد خوارزمية RSA في عملية التوقيع الرقمي على :
a. خوارزمية الهاش(تابع الهاش)

b. المفتاحين العام والخاص للمرسل
c. المفتاح العام للمستقبل
d. كل ما سبق
e. (*)a. و b.

106- باستخدام خوارزمية RSA نريد توليد مفتاح عام لكيان ما يتم ذلك على فرض ما يلي أنه تم اختيار العددين الأوليين و هما P=7 , q=11 عندها يكون $\Phi(n)$ هو:
a. 77
b. 88
c. (*)60
d. 61
e. 72

107- لنفرض أنه تم اختيار المفتاح العام ليكون e=17 فإن المفتاح الخاص المناسب هو:
a - 12
b - 52
c - (*)53
d - 11
e - 39

108- اختر العبارة الصحيحة :
a. من الصعب جدا معرفة المفتاح الخاص من معرفة المفتاح العام
b. من غير الممكن معرفة النص الأصلي plain text من معرفة المفتاح العام و خوارزمية التشفير
c. التابع وحيد الاتجاه one way function عملية حسابه سهلة و لكن عملية عكسه صعبة جدا
d. عشوائية اختيار مفتاح التشفير في خوارزمية الجمل هي السبب في كونها أكثر أمانا من RAS
e. (*)كل ما سبق

109- بفرض لدينا n=5 فإن $\Phi(n)$ هو:
a. 1
b. 2
c. 3
d. (*)4
e. 5

110- و بناء على ذلك فإن Z_n^* هو :
a. {1,2,3,4,5}
b. {1,2,3,4}(*)
c. {2,3,4,5}
d. {0,1,2,3,4,5}
e. {0,1,2,3,4}

111- إذا كان لدينا عدد g ينتمي للـ Z_n^* و يحقق الجدول الموضح فإن الإعداد التي تولد الزمرة هي:

g	Order
1	1
2	4
3	4
4	2
5	2
6	1
7	4

a. 1
b. 2
c. 3
d. 2,3,7
e. (*)b. و c.

112- نعلم أن خوارزمية DES تملك أربعة مفاتيح ضعيفة بحيث إذا استخدمنا تابع التشفير على النص المشفر اعتمادا عليها مرتين نتج لدينا النص الأصلي أي لدينا في حال كان بين أيدينا نص مشفر بواسطة إحدى هذه المفاتيح نطبق تابع التشفير على النص المشفر كحد أعلى 4 مرات و إحدى هذه المفاتيح هي:
a. $0101\ 0101\ 0101\ 0101_{16}$
b. $FEFE\ FEFE\ FEFE\ FEFE_{16}$
c. $1F1F\ 1F1F\ 0E0E\ 0E0E_{16}$
d. $E0E0\ E0E0\ F1F1\ F1F1_{16}$
e. (*)كل ما سبق

khaledyassinkh@gmail.com

113- نعلم أن خوارزمية DES تملك ست مفاتيح شبه ضعيفة كل مفتاح عبارة عن زوج من المفاتيح و المطلوب كم احتمال يلزمنا كحد أعلى في حال استخدام هذه المفاتيح وكان بين أيدينا نص مشفر بإحدى هذه المفاتيح:

a. (*)12
b. 6
c. 18
d. 14
e. 20

114- - نعلم أن خوارزمية DES تملك ست مفاتيح شبه ضعيفة كل مفتاح عبارة عن زوج من المفاتيح و المطلوب كم احتمال يلزمن كحد أدنى في حال استخدام هذه المفاتيح وكان بين أيدينا نص مشفر بإحدى هذه المفاتيح:

a. أقل من 12 محاولة
b. (*)أقل أو يساوي 12 محاولة
c. لا يمكن معرفة ذلك
d. 12 محاولة
e. لا يوجد

115- طول مفتاح التشفير في خوارزمية DES:

a. 56 bits b. 7 bytes c. 168 bits d. 221 bits e. (*)a. و b.

116- طول مفتاح خوارزمية 3DES هو:

a. 168 bits b. 21 bits c. 21 bytes d. 221 bits e. (*)a و c.

117- طول كتلة التشفير في خوارزمية DES هو:

a. 8 bytes
b. 64 bits
c. 128 bits
d. (*)a. و b.
e. a. و c.

118- طول كتلة التشفير في خوارزمية 3DES هو:

a. 192 bits
b. 24 bytes
c. 64 bits(*)
d. a. و c.
e. a. و b.

ملاحظة: نحن نعلم أن خوارزمية 3DES عبارة عن DES لكن ثلاث مرات هذا يعني أن الكتلة ستدخل إلى الخوارزمية بالمفتاح الأول و الناتج سوف يدخل إلى الخوارزمية بالمفتاح الثاني و الناتج سيدخل إلى الخوارزمية بالمفتاح الثالث أي أن الكتلة بقيت كما هي لم يتغير حجمها فقط زاد عدد المفاتيح ثلاث أضعاف و كذلك أصبحت الخوارزمية أبطئ بثلاث مرات و أكثر أمانا بثلاث مرات

119- اختر العبارة الصحيحة:

a. الخوارزميات المتناظرة يفضل استخدامها لتشفير المعطيات الضخمة
b. الخوارزميات غير المتناظرة يفضل استخدامها لتشفير المعطيات الصغيرة الحجم
c. إدارة المفاتيح في التشفير المتناظر أصعب من التشفير غير المتناظر
d. (*)كل ما سبق
e. a. و b.

120- أي من الأهداف الأمنية تستطيع الحد من أضرار هجوم التحري (Snooping attack) عن المعلومات؟

a. التشفير b. التخويل c. التكاملية d. الوثوقية e. (*)a. و b.

121- أي من الخدمات الأمنية لا تُحقق عن طريق SSL record protocol:

a. Message authentication
b. Entity authentication(*)
c. Confidentiality
d. Integrity
e. a. و b.

122- إذا كنت تريد أن تصمم بنية أمنية لشبكة داخلية فيجب أن تبدأ بـ:
a. التهديدات و المخاطر
b. السياسة الأمنية
c. (*)الممتلكات الشبكية للمؤسسة
d. الآليات الأمنية
e. كل ما سبق

123- الأهداف الأساسية لأمن المعطيات:
a. Confidentiality
b. Integrity
c. Availability
d. (*)كل ما سبق
e. Validated

124- عند استخدام MAC(message authentication code) للرسالة(للطرد) فإن ذلك يحقق:
a. Entity authentication
b. Message authentication
c. Integrity
d. Confidentiality
e. (*)b. و c.

125- البروتوكول الذي قد يسبب هجوم رفض/حجب الخدمة Dos(denial of service attack) هو:
a. IP
b. ICMP
c. TCP
d. ARP
e. (*)كل ما سبق

126- أي من بروتوكولات SSL تثبت الخوارزميات التي تم الاتفاق عليها عند طرفي الاتصال (client وserver):
a. Ssl change cipher spec protocol(*)
b. Ssl handshake protocol
c. Ssl alert protocol
d. Ssl record protocol
e. كل ما سبق

127- - أي من الجمل التالية غير صحيحة:
a. تعتمد فعالية البحث الشامل على كلمة السر Exhaustive Password search على سرعة أداء الجهاز مصدر الخطر
b. تعتمد فعالية البحث الشامل على كلمة السر Exhaustive Password search على فضاء المفاتيح
c. (*)تعتمد فعالية البحث الشامل على كلمة السر Exhaustive Password search على فضاء الرسالة المشفرة
d. a. و b.

ملاحظة: طريقة Exhaustive Password search تعتمد على تجريب كل الاحتمالات الممكنة و هي تعتمد على سرعة الجهاز و فضاء تمثيل كلمة السر (الذي كلما كان أكبر كان عملية البحث أصعب) و عادة تتم حماية كلمة السر عن طريق تحديد عدد محاولات محددة فإذا تم الإخفاق في كتابة كلمة السر بعد هذه المحاولات يتم إغلاق نافذة كتابة السر أو يتم تجميد مربع الحوار بحيث لا نستطيع إدخال كلمة جديدة

128- أي من الخوارزميات التالية تعتبر stream cipher:
a. RC2 b. RC6 c. RC5 d. RC4(*) e. RSA

129- تهديد تسريب المعلومات Information leakage ينتهك الخدمة الأمنية:
a. Confidentiality(*)
b. Integrity
c. DOS(denial of service)
d. Authentication
e. a. و b.

130- تهديد انتهاك التكاملية Integrity violation ينتهك الخدمة الأمنية:
a. Confidentiality
b. Integrity(*)
c. DOS(denial of service)
d. Authentication
e. a. و b.

131- خدمة connection confidentiality تتوفر في الطبقة من معيار OSI المرجعي :
a. الأولى
b. الثانية
c. الثالثة
d. الرابعة و السابعة
e. كل ما سبق(*)

132- هناك مشكلة في block cipher أنه كان هناك كلمة تتكرر كثيرا في النص الأصلي فإنها بعد التشفير سيكون النص المشفر مشابه أيضا و يمكن للمخترق attacker أن يحلل و يستنتج أن هذه الكتل المشفرة هي جملة واحدة و المطلوب ما هو الحل لتجنب مثل هذا التكرار :
a. Stream cipher
b. أنماط التشغيل Mode of operation
c. CBC
d. (*)b. و c.
e. لا يوجد

133- عند تصفحك لموقع www.bbcarabic.com واكتشفت أن هناك تشويه في الموقع أنت تكون:
a. في نفس الموقع لكن هناك تشويه
b. في موقع آخر
c. تم تسميم DNS لموقع bbcarabic
d. (*)a. و c.
e. b. و c.

134- إذا كان لدينا أرجحيه حدوث الخطر(إمكانية استغلال نقاط الضعف) V1=0.1 و V2=0.5 والقيمة الممتلكة 100 و ليس لدينا أي معلومة مئوية عن نسبة تسكين الخطر و كان لدينا معرفة مؤكدة لإمكانية حدوث الخطر بنسبة 80% يكون إمكانية حدوث الخطر:
a. 12
b. 35
c. 60
d. 72(*)
e. 200

135- إذا كان لدينا أرجحيه حدوث الخطر 0.2 والقيمة الممتلكة 1000 و لدينا معلومة مئوية عن نسبة تسكين الخطر بنسبة 50% و كان لدينا معرفة مؤكدة لإمكانية حدوث الخطر بنسبة 70% يكون إمكانية حدوث الخطر:
a. 100
b. 160(*)
c. 60
d. 200
e. 320

136- أي من التالي لا يحقق Authentication :
a. MAC(message authentication code)
b. التشفير encryption
c. التوقيع الرقمي digital signature
d. Hash function(algorithm)(*)
e. c. و d.

137- يستخدم الهاش لتحقيق:
a. التكاملية(*) integrity
b. عدم النكران Non- repudiation
c. السرية confidentiality
d. a. و b.

e. a. و b. و c.

138- من الأنسب لوضع السياسة الأمنية:
a. المدير التنفيذي
b. مدير أمن المعلومات
c. رئيس القسم
d. مهندس أمن الشبكات
e. (*)لا يوجد
ملاحظة: السياسة الأمنية لوضعها موضع التنفيذ يشارك فيها جميع العناصر في المؤسسة فهي عملية متكاملة يشارك فيها الجميع حتى المستخدمين العاديين في المؤسسة.
139- أي من العبارات التالية لا تحققها تعريف خوارزمية AES:
a. يعتمد على أطوال مفاتيح متغيرة
b. (*)يتعلق زمن تنفيذ الخوارزمية بطول الكتلة المشفرة
c. عدد الدورات يتعلق بحجم المفتاح
d. يعتمد على أطوال مفاتيح مختلفة
e. طول كتلة التشفير 16 bytes
140- أي من التقنيات التالية تؤمن التكاملية و authentication و عدم النكران معاً:
a. MAC(message authentication code)
b. التشفير المتناظر asymmetric encryption
c. (*)التوقيع الرقمي digital signature
d. خوارزميات الهاش
e. c. و d.

141- أي من الإجراءات التالية لا تحققها خوارزميات التشفير المتناظر:
a. MAC(message authentication code)
b. (*)عدم النكران non- repudiation
c. التكاملية integrity
d. Authentication
e. c. و d.
142- أي من الخوارزميات التالية لا تحتاج إلى مفتاح تشفير أو مفتاح مشترك لتقوم بعملها:
a. MAC(message authentication code)
b. التوقيع الرقمي digital signature
c. El Gamal
d. SHA(*)
e. RSA
143- أي من الخوارزميات التالية تعطي التشفير ذاته للرسالة مهما اختلفت معاملات الدخل للخوارزمية:
a. AES
b. DES
c. EL Gamal
d. RSA(*)
e. جميع ما سبق
144- أي من الخوارزميات التالية يتضاعف فيها حجم النص المشفر ليصبح ضعفي النص الأصلي:
a. AES
b. DES
c. EL GAMAL(*)
d. IDEA
e. RSA
145- اختر العبارة غير الصحيحة:
a. تعتمد خوارزميات التشفير اللامتناظر على صعوبة حل بعض المسائل الرياضية
b. (*)ليس من الضروري في خوارزميات التشفير اللامتناظر أن يكون حجم المفتاح كبير
c. يعتمد الأمن في خوارزميات التشفير اللامتناظر على طول الكتلة التي يجب أن تكون كبيرة نوعا ما
d. جميع ما سبق

e. a و c.

146- عند الحاجة لتبادل المعلومات الضرورية بين كيانين فيجب أن نحقق ما يلي:
a. التكاملية
b. السرية
c. (*)وثوقية كيان
d. وثوقية رسالة
e. التشفير

147- بفرض أن الفيروس يستخدم التعمية للاختباء في أي جزء من الأجزاء التالية تتم عملية التشفير:
a. Replicator
b. Protected(*)
c. Payload
d. Trigger

148- في أي جزء من أجزاء الفيروس يمكن أن تحوي التعليمة delete *.doc:
a. Replicator
b. Protected
c. Payload(*)
d. Trigger

149- أي من الخوارزميات التناظرية التالية ليست block cipher:
a. RC5
b. RC4(*)
c. IDEA
d. AES
e. SAFER

150- أي من Malware تحتاج لبرنامج مضيف لكي تنتشر:
a. Trojan
b. Virus
c. Worm
d. (*)a. و b.

151- أي من Malware التالية تنتشر عن طريق تدني التوعية لدى المستخدم:
a. Trojan(*)
b. Virus
c. Worm
d. A و B

152- أي من Malware التالية تنتشر بشكل تلقائي دون الحاجة لبرنامج مضيف:
a. Trojan
b. Virus
c. Worm(*)
d. لا يوجد

153- أي من العبارات التالية لا تحققها Stream cipher:
a. طول مفتاح التشفير يكون عادة بطول النص المراد تشفيره
b. (*)تعتمد على وجود مفتاح سري ثابت
c. تعتمد على تغير مفتاح التشفير
d. المفتاح المستخدم في التشفير يستخدم لمرة واحدة
e. تابع التشفير بسيط جدا و هناك مشكلة حقيقية في إدارة المفاتيح (توزيع المفاتيح)

154- ما هي مشكلة stream cipher:
a. السرعة في التنفيذ
b. تغير مفتاح التشفير
c. (*)يجب أن يكون هناك تزامن بين المرسل والمستقبل
d. تابع التشفير بسيط
e. مفتاح التشفير يستخدم لمرة واحدة

152- أي من العبارات التالية لا تشكل جزءاً من سياسة أمنية:

a. يجب تدريب العاملين على آخر التقنيات الحديثة
b. (*) استخدام Authentication للوصول إلى مخدم الطباعة
c. يجب أن يكون طول مفتاح التشفير في خوارزمية AES هو 256 bit حصرا
d. يجب الوصول إلى مخدمات الشبكة الداخلية من قبل مدير فقط
e. Aو B

153- أي من العبارات لا تعكس تعريف السياسة الأمنية :
a. السياسة الأمنية هي من مجموعة من القواعد توصف مسؤولية الشبكة
b. (*) السياسة الأمنية تقدم لنا الخدمات الأمنية من authentication و التشفير(السرية) و التكاملية
c. السياسة الأمنية تحد السلوك الأمني
d. السياسة لأمنية تحدد ما هو مسوح و ما هو ممنوع
e. السياسة الأمنية تطبق ضمن مجال معين

153- تحت 'أي نوع من أنواع الهجوم يمكن أن نصنف "قراءة المعلومات بطريقة غير شرعية":
a. المقاطعة Interruption
b. (*)الاعتراض أو التفتيش Interception
c. التعديل Modification
d. انتحال الشخصية Masquerade
e. النكران repudiation

154- تحت أي نوع من أنواع الهجوم يمكن ن نصنف "قيام المرسل بالإدعاء عدم قيامه بإرساله الرسالة":
a. المقاطعة Interruption
b. الاعتراض أو التفتيش Interception
c. التعديل Modification
d. انتحال الشخصية Masquerade
e. (*)النكران repudiation

155- تحت أي نوع من أنواع الهجوم يمكن أن نصنف "إلحاق الضرر بكابلات الشبكات":
a. (*)المقاطعة Interruption
b. الاعتراض أو التفتيش Interception
c. التعديل Modification
d. انتحال الشخصية Masquerade
e. النكران repudiation

156- تحت أي نوع من أنواع الهجوم يمكن أن نصنف "تأخر وصول الرد من قاعدة المعطيات"
a. (*)المقاطعة Interruption
b. الاعتراض أو التفتيش Interception
c. التعديل Modification
d. انتحال الشخصية Masquerade
e. النكران repudiation

157- عندما يكون النظام قد تعرض لهجوم المقاطعة فهذا يعني:
a. (*)أن النظام أصبح خارج الاستخدام
b. أن تتوفر التوافرية للشخص المخول
c. يستطيع الوصول للخدمات الأشخاص المخولين عند الحاجة
d. الوصول للخدمات تتم عن طريق التحكم بالدفق(النفاذ)

158- الهجوم الذي لا يمكن مواجهته بسهولة هو:
a. (*)هجوم رفض/حجب الخدمة DOS b. تشويه الموقع c.حذف المعطيات d. سرقة المعطيات

159- تحت أي نوع من أنواع الهجوم يصنف "قيام شخص غير مخول بالدخول إلى النظام كشخص مخول":
a. المقاطعة Interruption
b. الاعتراض أو التفتيش Interception
c. التعديل Modification
d. (*)انتحال الشخصية Masquerade
e. النكران repudiation

160- أي من الخوارزميات التالية التالية تعتبر خوارزميات لا تناظرية:
a. RSA
b. DES

c. AES
d. ELGAMAL
e. (*)a. و d.

161- أي من العبارات التالية غير صحيحة:
a. Mobile Code تشكل خطرا على مخدم الويب (web server)
b. الكود المتحرك Mobile Code هو كود تنفيذي
c. يمكن لبرنامج أن يشكل خطرا على مخدم الويب (web server)
d. الـ cookies تشكل خطرا على مخدم الويب (web server)
e. (*)a. و d.

162- أي من العبارات التالية تشير إلى تهديد أمني :
a. حصول Bug في البرنامج
b. عدم تعمية البيانات المنقولة عبر وصلات الشبكة أو الشبكة
c. لا يوجد مضاد فيروس
d. (*) النفاذ غير المخول من الشبكة الداخلية إلى شبكة الإنترنت
e. ترك بوابات شبكية مفتوحة

163- أي من العبارات التالية تشير إلى نقطة ضعف أمنية:
a. أن تكون Security training غير مناسبة للموظفين
b. وجود فيروسات
c. عدم وجود سياسة أمنية security policy
d. احتيال صفة شخص ما (انتحال شخصية)
e. (*)a. و c .

164- أي من العبارات التالية تشير إلى نقطة ضعف أمنية:
a. كلمات السر موضوعة ضمن الحاسب بطريقة غير محمية
b. شخص نسي إغلاق باب الغرفة التي تحوي المخدمات و المبدلات في الشركة
c. عدم إعداد الجدار الناري بشكل مناسب
d. (*)كل ما سبق
e. a. و c.

165- أي من Malicious software لا تحتاج لبرنامج مضيف:

a. Trojan Horse
b. Virus
c. Worm(*)
d. Trap door
e. Logic bomb

166- أي من العبارات التالية صحيحة:
a. التكاملية يؤمن خدمة السرية و التكاملية
b. (*) Authentication لا تؤمن حماية ضد إعادة إرسال الرسالة
c. التوقيع الرقمي يؤمن خدمة السرية
d. كل ما سبق
e. a. و c.

167- إذا كان كسر خوارزمية DES يتطلب 24 ساعة هذا يعني أن كسر خوارزمية 3DES يتطلب 3*24=72 hour حتماً فهل هذا صحيح؟
a. (*)ليس صحيح
b. صحيح
c. لا يمكن معرفة ذلك
d. لا يوجد

168- اختر العبارة الصحيحة:
a. تعتبر خوارزمية Diffe-Hellman من أهم الخوارزميات المستخدمة في عملية تبادل المفاتيح
b. يمكن تبادل المفاتيح بين المرسل و المستقبل فيزيائياً
c. يمكن تبادل مفتاح التشفير المتناظر باستخدام التعمية بالمفتاح العام للمستقبل
d. Aو B
e. (*)A و B و C

khaledyassinkh@gmail.com

169- اختر العبارة الصحيحة:
a. يمكن أن نستخدم التوقيع الرقمي بواسطة المفتاح العام للمرسل
b. يمكن ن نستخدم التوقيع الرقمي بواسطة المفتاح العام للمستقبل
c. يمكن أن يتضاعف النص الأصلي بمقدار الضعف تقريبا عند استخدام خوارزمية AES في التشفير
d. يمكن أن يتضاعف النص الأصلي بمقدار الضعف تقريبا عند استخدام خوارزمية 3DES في التشفير
e. (*)كل ما ذكر خاطئ

170- التشفير بشكل عام يؤمن:
a. التكاملية
b. السرية و الوثوقية
c. عدم نكران المرسل أنه مرسل الرسالة عن طريق تشفير هاش الرسالة (ملخص الرسالة) بالمفتاح الخاص للمرسل
d. (*)كل ما سبق
e. a. و b.

171- أي من الخوارزميات التالية يمكن أن تقبل أكثر من معاملين دخل :
a. EL GAMAL
b. RSA
c. AES
d. DES
e. **(*) جميع ما سبق**

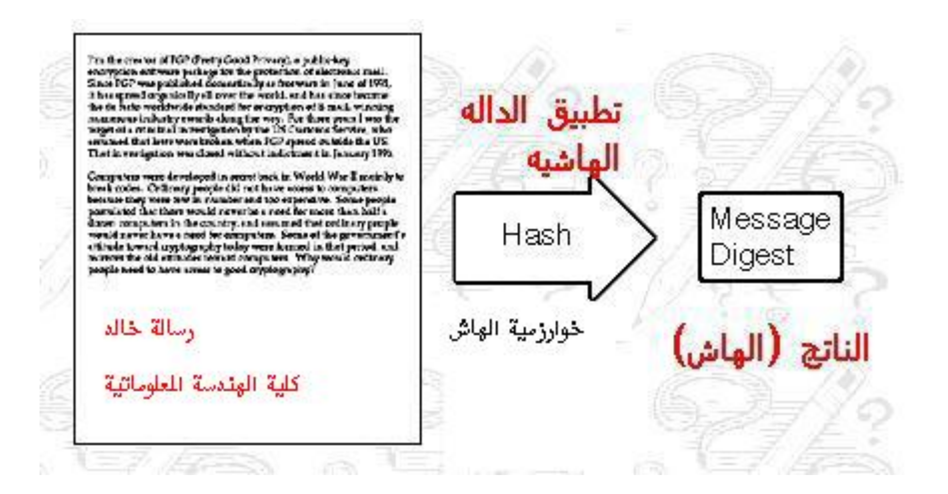
ملاحظة:

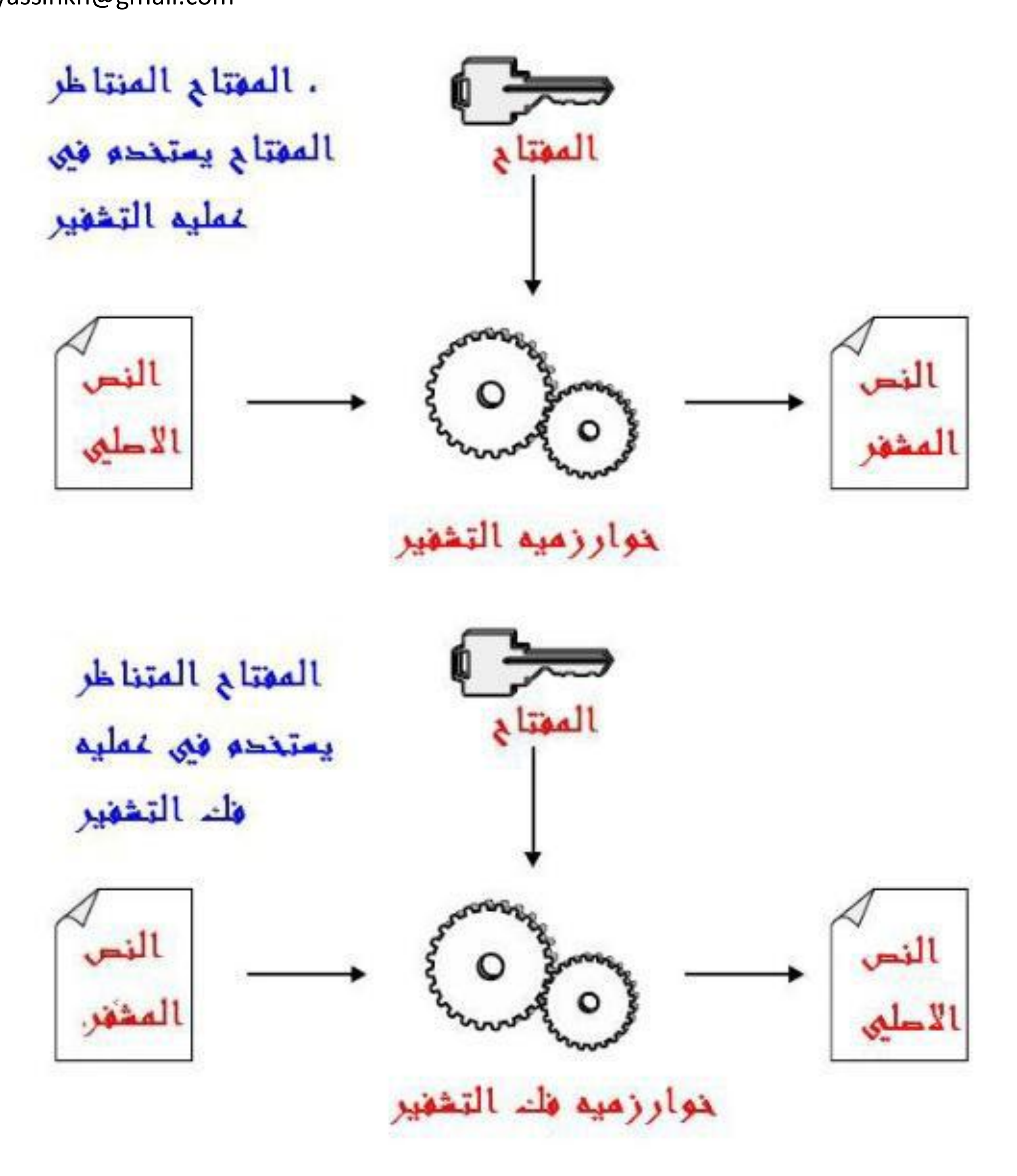
172- أي من الخيارات التالية لا تنتمي إلى مبادئ إدارة نظم المعلومات:
a. التخطيط planning b. السياسة policy c. people
d. الحماية protection **e.(*) القيادة Leading**

(و ما توفيقي إلا بالله)

ليس الموت هو الخسارة الكبرى..
الخسارة الكبرى.. هي ما يموت فينا و نحن أحياء

إن الطبيب له في الطب معرفة ما دام في آجل المريض تأخيرُ
حتى إذا انقضت أيام عدته حار الطبيب و خانته العقاقيرُ




. المفتاح المتناظر
المفتاح يستخدم في
عمليه التشفير
المفتاح
النص
الاصلي
النص
المشفر
خوارزميه التشفير
المفتاح المتناظر
يستخدم في عمليه
فك التشفير
المفتاح
النص
المشفر
النص
الاصلي
خوارزميه فك التشفير

khaledyassinkh@gmail.com

الرساله

TO: Sales Reps
FROM: VP
RE: Pricing

We're having a
slow quarter...

الكتله الاولى

TO: Sale

النص المشفر

j9%B8^cB

الكتله الثانيه

s Reps
F

النص المشفر

t&M0#'14~h

وهكذا حتى النهايه

الرساله

...
make those
sales!

الكتله الاخيره

es!

عمليه الحشو

es!1313131313131313131313131313

النص المشفر

.P3$h(j~

خوارزميه التشفير

النص الاصلي

Buy Acme
at $10

سلسله المفتاح

47 28 119 3
187 120 72 141
60 244 155 99
...

النص المشفر

9%jZR
+^-wv
...

khaledyassinkh@gmail.com



